EXPRESS MAIL LABEL NO.: EJ922406356US DATE OF DEPOSIT: May 31, 2000

I hereby certify that this paper and fee are being deposited with the United States Postal Service Express Mail Post Office to Addressee service under 37 CFR §1.10 on the date indicated above and is addressed to the Assistant Commissioner of Patents, Washington, D.C. 20231.

Dianne Lane
NAME OF PERSON MAILING PAPER AND FEE

Dianne Lane
SIGNATURE OF PERSON MAILING PAPER AND FEE

INVENTORS: Peter Bendel, Thomas Schaeck, and Roland Weber

S P E C I F I C A T I O N

Method and Apparatus for Controlling Access to the Contents of Web Pages by Using a Mobile Security Module

Sub a1

~~The present invention relates to a method and an apparatus for~~ controlling access to the contents of web pages by using mobile ~~security modules and in particular chip cards.~~

Sub a2

~~The internet, i.e. the World Wide Web, has become a new~~ information-disseminating and business medium. The increasing commercialization of the internet is constantly giving rise to ideas for new types of business which can be transacted over the

internet. Even today, the internet user can perform virtually all the commercial transactions involved in ordinary everyday life over the internet. In the business world too the internet has become an indispensable tool. Companies use the internet both for developing and for marketing their products.

However, there are also dangers to these opportunities offered by the internet. To an increasing extent, even confidential information is being exchanged between clients and servers over the internet. This is particularly true of the exchange of confidential knowhow. The client and the server therefore need to be sure that access to the confidential information is impossible while it is being transmitted over the internet. As well as this it must also be ensured that the authenticity of the receiver of the confidential information can be relied on. Finally, more and more providers of web servers are starting to restrict access to web contents, i.e. are permitting access only in return for the input of a user ID and password. In the prior art there are certain methods which have become established of guaranteeing authenticity between client and server and of ensuring that no unauthorized access is possible during transmission.

Prior art

Where access to web pages is restricted by means of a user ID and password, the browser is told that this is the case and it then opens a dialog box to allow a user ID and/or a password to be entered. Once the user ID and password have been entered, the browser sends them to the web server and if they are correct the latter opens access to the web pages.

A disadvantage of this method lies in the allotting and management of the user ID's and passwords and the possibility thereby created that the user ID's and passwords may be misused by unauthorized persons or may be listened in on by such persons when they are being transmitted from the client to the web server.

In an improved method the web server stores the client's TCP/IP address in a table. The TCP/IP address is thus considered to be authorized. A disadvantage of this method is that the TCP/IP address of the authorized client can be replaced by another TCP/IP address belonging to an unauthorized client if the unauthorized client has covertly found out the user ID and password. When this is the case the unauthorized person can still again access to the web server.

SSL (secure socket layer) is a transmission protocol for the secure transmission of information. Contemporary browsers largely support this protocol. Browsers which support SSL contain a database

holding certificates for public keys. Each public key is certified by a certificate issued by a recognized certification center. The protected-access web server contains a private key, with one public key being assigned to each such private key. For the public key in question, there is also a certificate on the web server.

The web server sends the certificate to the client. The certificate comprises the public key, identity data and a signature. The signature was generated by the web server by means of the private key. The client checks the validity of the certificate by reference to the certificates held in store and generates a signature by using an encryption algorithm and the public key. If the signature in the certificate is the same as the signature generated, the server has authenticated itself.

The same method can also be used to authenticate the client.

In this case too it is essential for the client to have a private key and a certificate.

The private key must be protected against access. Therefore it must not be stored on the client's hard disk. As an alternative to this the private key can be stored on a card. What is a disadvantage in this case however is that the card has to be capable of performing

a public key procedure and to do this it requires a cryptographic co-processor. This however makes the card expensive.

To provide a secure channel for communications, the SSL protocol makes it possible for the information for transmission to be encrypted by means of a session key on which the client and the web server have agreed. The session key is a symmetrical key. It is used to encrypt the information which is going to be transmitted.

Sub a3

~~The object of the present invention is to provide a method and an~~ apparatus which avoid the disadvantages, as outlined above, of the ~~prior art for achieving authentication between client and server.~~

Sub a4

~~This object is achieved~~ by means of the features described in ~~present invention are described in the subclaims.~~ claims 1, 15, 17, 18 and 20. Other advantageous embodiments of the

The main advantage of the present invention lies in the fact that the control of access to web pages in accordance with the invention does not require any changes to existing browsers. Also, the use of a chip card increases the security of the method of authentication employed in the present case.

Sub a5

~~The present invention will be described by reference to a preferred~~ embodiment and to drawings, in which

Fig.1 shows the components on which the present invention is based, and

Fig.2 shows the method according to the invention for ~~authentication and access control.~~

Sub a6

~~Fig.1 shows the components for implementing the present invention.~~ Installed on the client side there are a data-processing unit with a browser, a card reader and a mobile security module, e.g. a chip card. The browser is capable of displaying HTML pages and of running applets in its virtual machine (JVM = Java virtual machine). Applets are programs written in the Java programming language which are downloaded from the web server together with the web page. The function which the applets perform is to communicate with the chip card, e.g. by using APDU's (= application protocol data units). To communicate with the card, the applet requires a program library. This is necessary because communication is not one of the browser's standard functions. The chip card needs to be capable of calculating a cryptographic checksum or generating a digital signature by means of a key. The key is located in a protected area of the chip card. In addition to this, the ~~individual number of the card is preferably also stored on it.~~

On the server side there is a web server or data-processing unit which can handle HTTP requests from the client (an HTTP server).

The server is also capable of calling up not only static HTML pages but also programs (CGI = common gateway interface) or servlets. Servlets are programs written in Java which are used on web servers. The function which the servlets perform in the present invention is to verify the cryptographic checksum (or digital signature) generated on the client's side and thus to warrant the authenticity of the client to the web server.

The web server may have a protected area which is only accessible via an access control and an unprotected area to which access can be gained without access control.

The client and web server are connected via a data-carrying connection, e.g. the internet or an intranet, and communicate by means of a standard transmission protocol, e.g. TCP/IP.

To obtain a further increase in the security of the method, according to the invention, against snooping, SSL (secure sockets layer) is proposed as the transmission protocol.

The procedural sequence for the method according to the invention of controlling access to protected web pages on a web server is shown in detail in Fig.2. The method according to the invention comprises the following steps:

1. By entering a URL (uniform resource locator), the client requests a protected web page on a web server (HTTP request for page X). This request from the client causes a servlet to be started on the web server. By referring to a list, the servlet checks whether the URL contains a valid session ID as a parameter. A session ID is a prerequisite for access to a protected web page. If the session ID is included in the list, the process continues as detailed in step 10 below. If it is not (if this is an initial contact), authentication begins as detailed in step 2.

2. The servlet sends to the client an authentication page which contains an authentication applet. The authentication applet is parametrized with a random number which was generated by the servlet and with the URL address of the page originally requested (HTTP request for page X). The authentication applet is preferably stored in the client's volatile memory and run or activated by the browser.

3. The applet asks the user to identify himself by means of a chip card and initiates communication with the chip card, preferably by means of APDU's. The applet transmits the random number to the chip card.

4. Using a key which is stored in the protected area on the chip card, the card calculates a cryptographic checksum or digital

signature from the random number and its own card number. The checksum/digital signature and the card number are sent back to the applet.

5. The applet then makes a connection to the servlet on the web server and passes this data to the servlet.

6. The servlet checks to see whether the cryptographic checksum/signature is correct using a key which matches the chip card. Where the encryption process is symmetrical, the servlet is in possession of the same key; where it is asymmetrical, the servlet is in possession of the public key.

a) If the check sum does not agree, the servlet sends a negative answer to the applet. The applet shows the user an error message.

b) If the checksum is correct, the servlet generates a unique session ID from a large range of values to prevents its being discovered by a targeted search made by an unauthorized person.

The session ID is preferably provided with an expiry date and is entered in the servlet's list of valid session ID's. The session ID shows that the user in question is an authorized user for all requests within the session. The session ID loses its validity when:

- a fixed period has expired,
- the session is terminated by means of a log-off page.

7. The session ID is transmitted by the servlet to the applet. The applet preferably confirms the successful authentication.

8. At the end of step 7 of the method, the applet has the following information available to it:

- the URL address for page X, as originally requested, from step 3
- the session ID from step 7.

From this information the applet generates a new URL, with the new URL comprising the original address and the session ID, and transmits it to the browser. The applet has thus completed its duties.

9. The browser requests the web page in question from the web server.

10. The request for page X causes the servlet to be called up in the server. The servlet checks for the presence of the session ID in the URL as described in step 1. If the session ID is present, the servlet checks to see whether it is contained in the list and,

if it is, to see whether a validity date, if it has one, has expired.

If all the requirements for access are satisfied, the web page requested is loaded into the memory of the web server and processed. In the course of the processing, the web page in question is searched for any links to other web pages located in the area to which access is controlled. If any links of this kind are found, the user's session ID is added to them. It is preferable for an additional link for terminating the session, which also contains the session ID, to be inserted at the end of the page which was called up (see step 13).

11. The servlet transmits the page, with the modified links, to the client.

12. If, on the page displayed, the user follows a link which points to the protected area, this link will already include the session ID needed for authentication and this page will therefore be transmitted to the client without any renewed authentication as in step 2 et seq.

13. Events which specifically terminate the session and cause the session ID to be lost are:

- selection of the link for logging off (see step 10)
- expiry of the period of time for which a session ID has been allotted.

14. The servlet receives the log-off request from step 13 and deletes the session ID contained in the log-off request from the list of valid session ID's. The servlet preferably confirms to the user that the session is over.